PCT

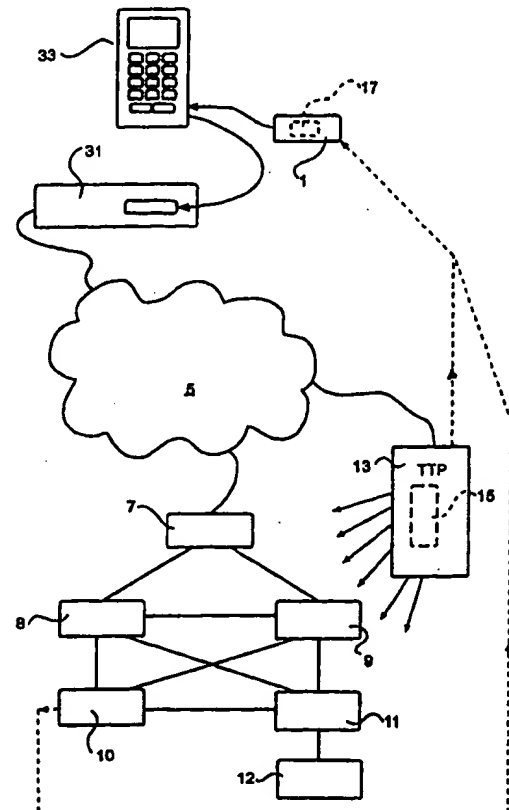## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification [6] :		(11) International Publication Number:	**WO 98/52151**
G06K 19/00, G07F 19/00, 7/10, H04L 9/32, 9/30	**A1**	(43) International Publication Date:	19 November 1998 (19.11.98)

(21) International Application Number: PCT/SE98/00897

(22) International Filing Date: 14 May 1998 (14.05.98)

(30) Priority Data:
9701814-7   15 May 1997 (15.05.97)   SE

(71) Applicant (for all designated States except US): ACCESS SECURITY SWEDEN AB [SE/SE]; Mariebergs Säteri, S–147 92 Grödinge (SE).

(72) Inventor; and
(75) Inventor/Applicant (for US only): SJÖBLOM, Hans [SE/SE]; Vårgårdsvägen 51, S–133 36 Saltsjöbaden (SE).

(74) Agent: AWAPATENT AB; P.O. Box 45086, S–104 30 Stockholm (SE).

(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
In English translation (filed in Swedish).

(54) Title: ELECTRONIC TRANSACTION

(57) Abstract

A method and a device for carrying out electronic transactions. A sender produces, under his own full control, a transaction message in a smart card (1) and provides the message with his digital signature in the card for subsequent output and transmission.

1

ELECTRONIC TRANSACTION

Field of the Invention

The present invention relates to electronic trans-
actions, i.e. primarily payments, which are effected
electronically. More specifically, the invention con-
cerns electronic transactions effected while employing
a user card, such as a cash card, credit card, charge
card, or the like, said card being a so-called smart
card.

Background Art

In recent years, the interest in electronic trans-
actions has increased significantly, especially concur-
rently with the impact of the Internet. Security matters
have been focused, and different systems and standards
have been suggested to guarantee the security in connec-
tion with electronic transmission of transaction mes-
sages. A matter that has attracted a lot of interest is
how to protect, for instance, credit card numbers trans-
mitted via the Internet in connection with Internet shop-
ping. What the systems and standards proposed have in
common is that they are based either on the condition
that sensitive information that may be misused, for in-
stance a credit card number, is not to be transmitted via
the communications network, or on the condition that such
sensitive information is to be transmitted in encrypted
form. In both alternatives, the relatively complicated
administrative routines and system configurations etc.
are focused, which, as will be appreciated, results in
restrictions and obstacles to a more general use.

Objects of the Invention

A main object of the present invention is to faci-
litate electronic transactions in a simplified fashion
while maintaining full security.

A further object is to facilitate different kinds
of electronic transactions within the scope of the same
basic concept.

2

One more object is to facilitate electronic trans-
actions independently of the choice of information trans-
fer channel for the used transaction message.

A still further object is to facilitate electronic
5   transactions which basically do not require transmission
of the used transaction message through a reliable infor-
mation transfer channel.

Summary of the Invention

The above-mentioned objects are achieved by the
10   inventive features that are stated in the accompanying
claims.

The invention thus is based on an insight of the
advantage of using special transaction messages which,
independently and under the user's full control, are
15   created by a user and which are of such nature that they
can have been created by the user only, they cannot have
been tampered with while being transferred to a receiver
or addressee without such tampering being easily recog-
nised (authentication) and can easily be validated after
20   transfer for the purpose of finalising the desired trans-
action. According to the invention, the sender uses a
unique smart card assigned to him, with a private key
stored therein (whose public equivalence in an asymmetri-
cal cryptographic system is generally available) in order
25   to provide a transaction message created by the sender
with a digital signature which is unique to the sender,
whereupon the signed transaction message can be trans-
ferred in an arbitrary manner.

Only a lawful user of the smart card can activate
30   this to be signed, thereby satisfying a basic identity
requirement. The digital signature further entails a data
lock which prevents the message from being tampered with
without this being recognised in a subsequent authentica-
tion by using the generally available public key, which
35   belongs to the user. The user's independent creating of
the transaction message means full control of the con-
tents of the message. The invention thus requires that

3

sensitive information, such as a card number, in the
transmitted transaction message be connected to a digital
signature to make the information at issue usable. With-
out connection to a digital signature, the information
5   thus is basically of no value and consequently cannot
be misused for false network transactions, even if the
information could be caught by a person not concerned in
connection with a transmission of the transaction mes-
sage. Basically, it is irrelevant how the transmission
10 takes place. This means an approach which is completely
opposite to today's striving for the provision of spe-
cial, reliable, i.e. encrypted, communication systems for
transmitting transaction messages via e.g. the Internet.

It is preferred that a transaction message according
15 to the invention contains information on sender, trans-
action amount and receiver and preferably a variable
piece of information, such as a serial number.

According to the invention, the user thus creates
what can be said to be a signed "electronic cheque",
20 which can be transmitted in an arbitrary manner and at
an arbitrary point of time to an addressee or receiver.

Upon receipt, a transaction message according to the
invention can be checked for authenticity by checking the
digital signature, whereupon validation and charging or
25 crediting the receiver with the transaction amount at
issue can take place in an arbitrary, suitable manner,
suitably according to the same principles as apply to the
cashing of an ordinary cheque or to clearing in connec-
tion with a card purchase.

30 According to the invention, the transmitted, signed
transaction message may contain the required transaction
information as plain text, in which case the digital sig-
nature can, in a manner known per se, be provided on the
basis of a condensate of the message information. This
35 means that the subsequent authentication, validation and
crediting on the receiver side will be facilitated since
the required information is immediately available, such

4

as information on sender, which makes it easy to fetch
the correct public key for authentication of the digital
signature.

If the digital signature is effected on the entire
5   transaction message such that this is transmitted in
encrypted form, the transmitted transaction message can
be provided with special sender information which makes
it possible on the receiver side to fetch the correct
public key for authentication and conversion of the
10   transaction message into plain text.

According to the invention, the transaction message
may contain sender information of an arbitrary, suitable
kind, such as at least one of the following pieces of
information: a card number, a cash card number, a charge
15   card number, a credit card number, an account number, an
invoice number and an ID number. If the smart card uti-
lised according to the invention is a card connected to
an account, such as a credit card, it may be preferred
to use the associated card number as sender information.
20   As those skilled in the art realise, it is however pos-
sible to use any kind of information, which on the re-
ceiver side can easily be connected to a user identity
and, consequently, to an associated account which is to
be charged.

25   For the receiver information, basically the same
applies. For instance, at least one of the following
pieces of information may be involved: a card number,
a cash card number, a charge card number, a credit card
number, an account number, an invoice number and an ID
30   number. Also in this case, it is sufficient that the
information on the receiver side can be unambiguously
related to a receiver of payment. It should be noted that
transferring a transaction amount to a receiver need not
entail the crediting of a receiver account, but it may
35   also imply that e.g. an administrative unit receiving the
transaction message, after authentication and validation,

5

charges a sender account and sends to the receiver what
may be considered a check or a postal order.

As described above, an essential feature of the pre-
sent invention is that the sender, i.e. the user of the
5   smart card, creates and signs the transaction message
under his own control, i.e. basically independently of a
connection to a communications network and of a computer
dialogue with a receiver, although such a dialogue of
course may take place in connection with the transmission
10 of a signed transaction message. Consequently the trans-
action message is created preferably without connection
to the communications network or off-line. This means
that the sender fully controls which data are input for
creating of the transaction message. As will be appre-
15 ciated, the signing can be carried out only by the sender
since in the normal case he is the only one to be able
to activate his smart card and to release the signing.
Regarding the transmission or handing over of the signed
transmission message there are, however, no restrictions,
20 as will be quite easily appreciated. For example, the
user or some person assisting him may take the smart card
with the signed transaction message present therein to
send the message later, to send the message from some
other place etc, that is to say there is a great freedom
25 of choice. The signed transaction message could also be
transferred to special intermediate materials or a
transport medium to be transmitted to a receiver and/or
addressee.

According to the invention, it is advantageous that
30 the transaction message is created in the smart card. The
transaction message may suitably be created by means of
the software inserted in the smart card in advance and
sender information preferably inserted in the card in
advance, e.g. a card number. Suitably a new serial num-
35 ber is automatically created for each transaction mes-
sage. The input of the necessary message information in
the card may be carried out in different ways, for in-

6

stance with the aid of the input means arranged on the
smart card, the card advantageously consisting of a so-
called advanced smart card. Information that is required
for the transaction message can also be input with the
5   aid of a protected card terminal, which advantageously
may consist of the user's own terminal or computer pro-
vided with a card reader. Information that is necessary
for the transaction message can also be input by means
of a separate card communication unit, the latter prefer-
10   ably later also serving as card activator. Such a unit
can advantageously be designed as a small portable unit,
which the user may take along and which is utilised by
the user when he wants to activate his card and/or input
information in the card in surroundings where no protect-
15   ed card terminal is available.

Information which is required for the transaction
message can also be input by means of a telecommunica-
tions unit controlled by the smart card, especially a
mobile telecommunications unit, such as a mobile tele-
20   phone device. In this context, the unit may also be used
to transfer the signed transaction message, for instance
by using a so-called SMS-type service.

The man skilled in the art realises that it is also
possible to create the actual transaction message outside
25   the smart card by using, for instance, one of the above-
mentioned information input means. The created trans-
action message is then input in the smart card to be
signed.

According to a first aspect of the present inven-
30   tion, a method is provided for carrying out electronic
transactions, in which a sender of transaction messages
is assigned a smart card with an associated unique iden-
tity and a private key stored in the card in a protected
manner, and in which an associated public key is kept
35   generally available, said method being characterised in
that in connection with an electronic transaction under
the sender's own control, preferably through his own

7

input of message information, the sender creates a trans-
action message, which contains information necessary for
the transaction, and, in his smart card, provides the
created transaction message with his digital signature
5   while using his own private key for the purpose of subse-
quent output and transmission of the transaction message.

According to a second aspect of the present inven-
tion, a smart card is provided for carrying out electro-
nic transactions, said card comprising means for storing
10 of card identification information, means for protected
storing of a private key, means for storing of an asymme-
trical algorithm, means for input of transaction informa-
tion into the card, processor means for creating in the
card a transaction message based on input transaction
15 information, such as information on amount and receiver,
and optionally information stored in the card, such as
information on sender and preferably a serial number, and
for providing the transaction message with a digital sig-
nature on the basis of said private key and said asymme-
20 trical algorithm, and means for output of the signed
transaction message.

According to a third aspect of the present inven-
tion, a combination is provided of a smart card and a
user-controlled communication unit, which is arranged for
25 communication with the smart card and with which the card
is adapted to be combined with a view to producing an
electronic transaction message, the card comprising means
for protected storing of a private key, means for storing
of an asymmetrical algorithm and processor means for pro-
30 viding a created transaction message with a digital sig-
nature based on said private key and said algorithm, and
said communication unit comprising means for input of
transaction information, and means being arranged in the
communication unit and/or in the card for producing said
35 transaction message.

A fourth aspect of the present invention involves
use of a smart card with a private key stored therein and

8

asymmetrical cryptographic algorithm for providing in the card, independently of the communications network, an electronic transaction message provided with a digital signature based on the private key.

5   Additional aspects of distinctive features of the invention will appear from the following detailed description of various embodiments with reference to the accompanying drawings.

Brief Description of the Drawings

10   Fig. 1 is a schematic illustration of an example of the carrying out of electronic transactions by using an open network, such as the Internet, in accordance with an embodiment of the present invention.

Fig. 2 is a schematic illustration of the same kind

15   as in Fig. 1, exemplifying alternative ways of carrying out electronic transactions according to the invention.

Fig. 3 is a schematic illustration of an example of the carrying out of electronic transactions by using a shop card terminal, according to a different embodiment

20   of the present invention.

Fig. 4 is a schematic illustration of the same kind as in Fig. 3 of another example of the carrying out of electronic transactions by using a shop card terminal, according to the present invention.

25   Fig. 5 is a schematic illustration of an example of the carrying out of electronic transactions by using a mobile telephone system, according to one more embodiment of the present invention.

Fig. 6 is a schematic illustration of an example of

30   the carrying out of electronic transactions by using an open network for direct contact with a bank, according to another embodiment of the present invention.

Fig. 7 is a schematic illustration of examples showing how an advanced smart card can be used to carry out

35   electronic transactions in accordance with the present invention.

Description of Embodiments

Fig. 1 illustrates schematically a first embodiment
of the invention, which can be used for credit card pay-
ment via an open network, such as the Internet, between
5   a sender and a receiver included in a network. The sender
has access to a smart card 1 and a computer 3 which is
provided with a suitable card reader (indicated at 2),
and which typically can be a home computer and is con-
nected to the Internet 5. A network server 7 is connected
10   to the network 5 and to various credit card administra-
tors 8 and 9 included in the network. The latter are in
conventional manner connected to each other and to
various institutions keeping accounts, such as banks 10,
11. In the present example, the sender is supposed to
15   have an account in the bank 10 and a credit card admi-
nistered by the administrator 8, while the receiver 12
has an account in the bank 11 and a credit card adminis-
tered by the administrator 9.

A trusted third party (TTP) 13 is network admini-
20   strator and responsible for the necessary handling of
keys. TTP 13 thus assigns to each user his private key
which is stored in a protected manner in the user's card
1, and keeps a catalogue 15 available, from which the
public key of each user can be collected.

25   The user's smart card 1, which also has a conven-
tional credit card function, contains in a known manner
memory and processor means in the form of one or more
integrated circuits (indicated at 17), as well as con-
ventional means for enabling communication between the
30   card and a card reader when the card is placed in the
latter.

In addition to the above-mentioned private key, said
memory and processor means contain a cryptographic algo-
rithm of an asymmetrical type, which can be a DES algo-
35   rithm, and software for effecting the signing of a trans-
action message based on the private key and said crypto-
graphic algorithm. The smart card 1 is activated in an

10

arbitrary, suitable manner, for instance by means of a
PIN input in the card, or biometrically.

When performing a transaction, the card 1 is placed
in the card reader 17 of the computer 3 and the card

5   is activated if this has not already been done. A trans-
action message can now be created in the smart card 1
and/or in the computer 3. If the creation takes place
exclusively in the card, which from the viewpoint of
security may be preferred, the card also contains soft-

10 ware that is suitable for this purpose. In this case, the
required information for the transaction message (espe-
cially regarding amount and receiver) is input via the
keyboard of the computer 3 into the card.

If the actual transaction message is created in

15 the computer, this has been provided with the software
required for this purpose, which is suitably supplied to
the user in connection with the issuance of the smart
card. Also in this case, message information is input
via the keyboard.

20   It is advantageous to use as sender information a
card identification, such as the number of the smart
card, which is automatically supplied by the card as the
transaction message is being created. As receiver infor-
mation the card number of the receiver can advantageously

25 be input.

After creating the transaction message, it should be
provided with a serial number and signed, which, as men-
tioned above, is effected in the card. If the actual mes-
sage has been created in the card, it may be desirable,

30 with a view to restricting the software that must be
available in the card, to effect the digital signature on
the actual message, whereby the message obtains the form
of cryptographic text. The signed message which is then
transferred must be able to supply information on the

35 sender, thereby making it possible to collect the public
key necessary for authentication, as will be described
below. Especially if the transaction message is created

11

in the sender's own protected computer, it may be suitable to generate the digital signature on a condensate of the actual message, which will be available as plain text and also can be transmitted as plain text.

The signed transaction message can now advantageously be given the form of e-mail and then be transmitted via the network 5 to the network server 7.

If the transaction message is available as plain text, the server 7 can, based on the information in the transaction message, directly send the signed message either to the sender's or the receiver's card administrator 8, 9, respectively, for the purposes of authentication and, if authenticity has been established, subsequent validation, charging the sender and crediting the sender with the transaction amount involved, while applying a suitable clearing procedure.

The authentication means that, for instance, the sender's card administrator fetches the sender's public key from a key catalogue of his own or the catalogue 15 of TTP 13 and, by means thereof and of the cryptographic algorithm involved, checks the digital signature of the message.

If the message received by the server is not available as plain text, the server 7 fetches from the catalogue 15 the public key belonging to the sender who can be identified by the received, signed transaction message, e.g. on the basis of special sender information such as a network identity or Internet identity. After conventional decrypting of the message by using the fetched public key, the server 7 has access to the information of the message as plain text and can send the message on for authentication etc, as mentioned above.

One more alternative is to provide the message sent on the network 5 with a stated address of the authorised card administrator, for instance 8, such that the server can directly direct the message to him for continued processing as described above. If the signed message is not

12

available as plain text, the received message must also
in this case provide such information that the correct
public key can be fetched for authentication and decryp-
tion of the actual message.

5   Fig. 2 illustrates schematically a second embodiment
of the invention, which uses basically the same configu-
ration as in Fig. 1, although the transaction message
from the sender is transmitted directly to a receiver's
computer 21 via the network 5. The receiver sends the

10   message on, which can be carried out via the network to
the server 7, as indicated by the arrow 23, or by some
other route as indicated by the arrow 25.

        In this embodiment, it may be convenient that the
actual message is available as plain text, such that the

15   receiver can see the information therein even if he does
not have immediate access to the sender's public key for
authentication or decryption of the digital signature. If
needed, the signed message can however be encrypted by
the sender with a public key belonging to the receiver,

20   in which case the receiver upon receipt decrypts the mes-
sage by using his own private key and the associated
cryptographic algorithm and then forwards the decrypted,
but still signed message.

        In case of a transport route 25 other than the net-

25   work 5, it may be advantageous to use intermediate mate-
rials, for instance a disk (indicated at 26), which in
some suitable and reliable manner, the receiver hands
over to his card administrator or bank for continued pro-
cessing in accordance with that described above. It will

30   be appreciated that the receiver can collect a number of
received transaction messages on such intermediate mate-
rials before taking steps for the continued processing.

        Fig. 3 illustrates schematically an embodiment of
the invention which is suited for transactions via a

35   foreign "terminal" 31 and which uses a user-controlled
portable unit 33 for creating a transaction message.

13

The unit 33 consists of a combined activator and information inputting means for the smart card. The unit 33 is in a suitable manner arranged for communication with the card 1, for instance by comprising an integrated

5   card reader, into which the card is inserted. The unit 33 further has a keyboard and a display.

When paying in e.g. a shop, the card is inserted in the unit 33 and activated, for instance, by inputting a PIN code by means of the keyboard of the unit. By means

10   of the keyboard, the necessary payment information is also input, such as amount and receiver. If the transaction message is both created and signed in the actual card, the actual information will be transferred to the card. If the actual message and optionally a condensate

15   thereof are to be created in the unit 33 for the purposes of transferring to and signing in the card 1, the unit is provided with processor means and the software required for this purpose.

The card with the signed transaction message is now

20   removed from the unit 33 and inserted into the shop's reader/terminal 31, from which the message is transmitted for continued processing in the same manner as described above. Accepted authentication and validation may suitably result in a receipt being sent back to the terminal.

25   It will be appreciated that the terminal 31 could, of course, communicate with the server 7 in some other manner than via the network 5, for instance via a protected connection.

Fig. 4 illustrates a variant of the embodiment shown

30   in Fig. 3. The unit 33 in Fig. 3 is replaced by a protected, preferably off-line computer or terminal 43, which can be arranged in, for instance, a shop and permits off-line, secure creation of a transaction message in a way similar to that described in connection with

35   Fig. 3, for the purposes of input in a shop card terminal 31.

14

Fig. 5 illustrates an embodiment of the present
invention which involves the use of a mobile telephone
device 51 and an associated mobile telephone network 55.
The mobile telephone device comprises, in addition to a
5   mobile telephone function, also such an activating and
input function as described in connection with the unit
33 in Fig. 3. The mobile telephone function is preferably
also controlled by the smart card.

With the aid of the telephone function, the signed
10   transaction message is transmitted to a unit or central
unit 57, which effects continued processing of the trans-
action message, for instance, in accordance with that de-
scribed in connection with the preceding Figures.

The transmission of the transaction message can ad-
15   vantageously take place while using a so-called SMS ser-
vice or the like of the mobile telephone network.

The unit 57 could also be a special central unit,
which after authentication etc. effects payments based
on the received transaction messages.

20   Fig. 6 illustrates an embodiment of the present
invention which advantageously can be used to effect
payment orders. At a sender's, i.e. payer's place, signed
transaction messages are created as described, in this
case exemplified with the same method as in Fig. 1. The
25   transaction message is transmitted to the sender's bank
10 keeping the account, which in a catalogue 60 has
access to the sender's public key. It will be appreciated
that the bank could be card issuer and key administrator
and that the sender information in the transaction mes-
30   sage can suitably consist of the sender's bank account
number.

Upon receipt of a transaction message and authenti-
cation thereof, the sender's bank 10 provides for, by a
clearing procedure, the payee, who is identified in the
35   transaction message suitably by the associated bank
account number, being credited with the amount at issue,

15

i.e. the receiver's account in the receiver's bank 11
being credited with the amount at issue.

Another alternative possibility is that the sender's
bank 10 sends a delivery order directly to the receiver
5   12 based on, for instance, receiver information in the
transaction message. This alternative is indicated by
means of the dashed line 62 in Fig. 6.

In the embodiment according to Fig. 6 it may be con-
venient to encrypt the transmitted, signed transaction
10   message, thereby increasing the security. The sender then
uses the public key of the bank 10 and preferably the
same cryptographic algorithm as is used for signing. As
will be appreciated, the bank 10 can immediately carry
out decryption by using its private key.

15   If the bank 10 is administrator of the sender's pair
of keys, i.e. has both the public key and the private key
belonging to the sender, the sender can alternatively
carry out the encryption of the signed message with the
aid of his public key. The bank 10 can then decrypt the
20   transmitted message by using the sender's private key,
which is collected from a catalogue, before authentica-
tion is carried out by using the sender's public key.

Finally, Fig. 7 illustrates schematically the use
of a so-called advanced smart cart in connection with the
25   invention. The advanced smart card 71 also has a keyboard
and a display, which allows that a signed transaction
message can be created in the card completely without
external aids. Subsequently the card can be inserted into
e.g. a computer or a terminal for the purposes of for-
30   warding the message and continued processing in accor-
dance with that described above.

Although the invention has been illustrated by a
number of embodiments, the invention is of course not
restricted thereto, and changes and modifications are
35   feasible within the scope of the appended claims. Thus,
individual features from the various embodiments may
be brought together in new combinations within the scope
of the inventive idea.

16

CLAIMS

1.   A method for performing electronic trans-
actions, in which a sender of transaction messages is
assigned a smart card with an associated unique identity
and a private key stored in the card in a protected man-
ner, and in which an associated public key is kept gene-
rally available, c h a r a c t e r i s e d in that in
connection with an electronic transaction under the
sender's own control, preferably through his own input
of message information, the sender creates a transaction
message, which contains information necessary for the
transaction, and, in his smart card, provides the created
transaction message with his digital signature while
using his own private key for subsequent output and
transmission of the transaction message.

2.   A method as claimed in claim 1, c h a r a c -
t e r i s e d in that the transaction message contains
information on sender, receiver, amount and preferably
a transaction serial number.

3.   A method as claimed in claim 1 or 2, c h a r -
a c t e r i s e d in that the transaction message is
created off-line, i.e. not connected to the communica-
tions network that is used for the subsequent transmis-
sion of the transaction message.

4.   A method as claimed in claim 3, c h a r a c -
t e r i s e d in that the transaction message is created
off-line.

5.   A method as claimed in any one of the preceding
claims, c h a r a c t e r i s e d in that the transaction
message is created in the smart card.

6.   A method as claimed in claim 5, c h a r a c -
t e r i s e d in that the transaction message is created
with the aid of software inserted in the smart card in
advance and preferably also sender information inserted
in the card in advance.

17

7. A method as claimed in claim 5 or 6, c h a r -
a c t e r i s e d in that information required for the
transaction message is input with the aid of input means
arranged on the smart card, the card preferably being a
5   so-called advanced smart card.

8. A method as claimed in any one of claims 1-6,
c h a r a c t e r i s e d in that information necessary
for the transaction message is input with the aid of a
protected card terminal.

10   9. A method as claimed in any one of claims 1-6,
c h a r a c t e r i s e d in that information necessary
for the transaction message is input with the aid of a
separate card communication unit, the latter preferably
also being a card activator.

15   10. A method as claimed in any one of claims 1-6,
c h a r a c t e r i s e d in that information necessary
for the transaction message is input with the aid of a
telecommunications unit controlled by the smart card,
especially a mobile telecommunications unit such as a
20   mobile phone.

11. A method as claimed in any one of the preceding
claims, c h a r a c t e r i s e d in that the transaction
message contains sender information in the form of at
least one of the following pieces of information: a card
25   number, a cash card number, a charge card number, a cre-
dit card number, an account number, an invoice number and
an ID number.

12. A method as claimed in any one of the preceding
claims, c h a r a c t e r i s e d in that the transaction
30   message contains receiver information in the form of at
least one of the following pieces of information: a card
number, a cash card number, a charge card number, a cre-
dit card number, an account number, an invoice number and
an ID number.

35   13. A method as claimed in any one of the preceding
claims, c h a r a c t e r i s e d in that the signed
transaction message is sent to a card or account admini-

18

strator regarding the sender or receiver, that the digi-
tal signature of the transaction message is authenticated
by using the public key, which is assigned to the one who
is identified as sender by the transmitted transaction
5   message, and that in case of authenticity, the receiver
is credited with the transaction amount by a clearing
process.

    14.   A method as claimed in claim 13, c h a r a c -
t e r i s e d in that the signed transaction message is
10   first sent to the receiver, who optionally after his own
checking of the digital signature of the message forwards
the signed transaction message to said card or account
administrator.

    15   A method as claimed in any one of claims 1-12,
15   c h a r a c t e r i s e d in that the signed transaction
message is encrypted by using a public key belonging to
the addressee, to whom the transaction message is sent,
that the encrypted, signed transaction message is sent
to the addressee, that the addressee by using his private
20   key decrypts the signed transaction message, that the
digital signature of the transaction message is authenti-
cated by using the public key which is assigned to the
one who is identified as sender by the transmitted trans-
action message, and that the receiver, in case of authen-
25   ticity, is credited with the transaction amount by a
clearing process.

    16. A method as claimed in claim 15, c h a r a c -
t e r i s e d in that the addressee is the receiver, that
the receiver, after decryption, sends the signed trans-
30   action message to a card or account administrator, where-
upon said authentication takes place.

    17.   A method as claimed in any one of claims 1-12,
c h a r a c t e r i s e d in that the signed transaction
message is encrypted by using the sender's public key and
35   is provided with sender information and is then sent to a
card or account administrator, who has the sender's pri-
vate key and who preferably has issued the user's smart

19

card, that said administrator decrypts the received
encrypted message by using said private key, that authen-
tication of the digital signature of the decrypted trans-
action message takes place by using the public key, which
5   is assigned to the one who is identified as sender by the
transmitted transaction message, and that the receiver,
in case of authenticity, is credited with the transaction
amount by a clearing process.

18. A method as claimed in any one of claims 1-14,
10   c h a r a c t e r i s e d in that the signed transaction
message is sent non-encrypted, especially via a public
communications network, such as the Internet or a tele-
communications network.

19. A method as claimed in any one of the preced-
15   ing claims, c h a r a c t e r i s e d in that the signed
transaction message is sent by e-mail.

20. A method as claimed in any one of claims 1-18,
c h a r a c t e r i s e d in that the signed transaction
message is sent via a mobile telephone network, especial-
20   ly by using a so-called SMS service.

21. A smart card for carrying out electronic trans-
actions, comprising means for storing card identification
information, means for protected storing of a private
key, means for storing an asymmetrical algorithm, means
25   for input of transaction information into the card, pro-
cessor means for creating in the card a transaction mes-
sage based on input transaction information, such as
information on amount and receiver, and optionally infor-
mation stored in the card, such as information on sender
30   and preferably a serial number, and for providing the
transaction message with a digital signature on the basis
of said private key and said asymmetrical algorithm, and
means for output of the signed transaction message.

22. A card as claimed in claim 21, c h a r a c -
35   t e r i s e d in that it is of a so-called advanced type.

23. A combination of a smart card and a user-con-
trolled communication unit, which is arranged for commu-

20

nication with the smart card and with which the card is
adapted to be combined with a view to producing an elec-
tronic transaction message, the card comprising means for
protected storing of a private key, means for storing an
5 asymmetrical algorithm and processor means for providing
a created transaction message with a digital signature
based on said private key and said algorithm, and said
communication unit comprising means for input of trans-
action information, and means being arranged in the com-
10 munication unit and/or in the card for creating said
transaction message.

     24. A combination as claimed in claim 23,
c h a r a c t e r i s e d in that the communication unit
is a mobile telecommunication device.

15   25. A combination as claimed in claim 23,
c h a r a c t e r i s e d in that the communication unit
is a combined card activator and information inputter/
processor.

     26. Use of a smart card with a private key stored
20 therein for providing, independently of the communica-
tions network, an electronic transaction message provided
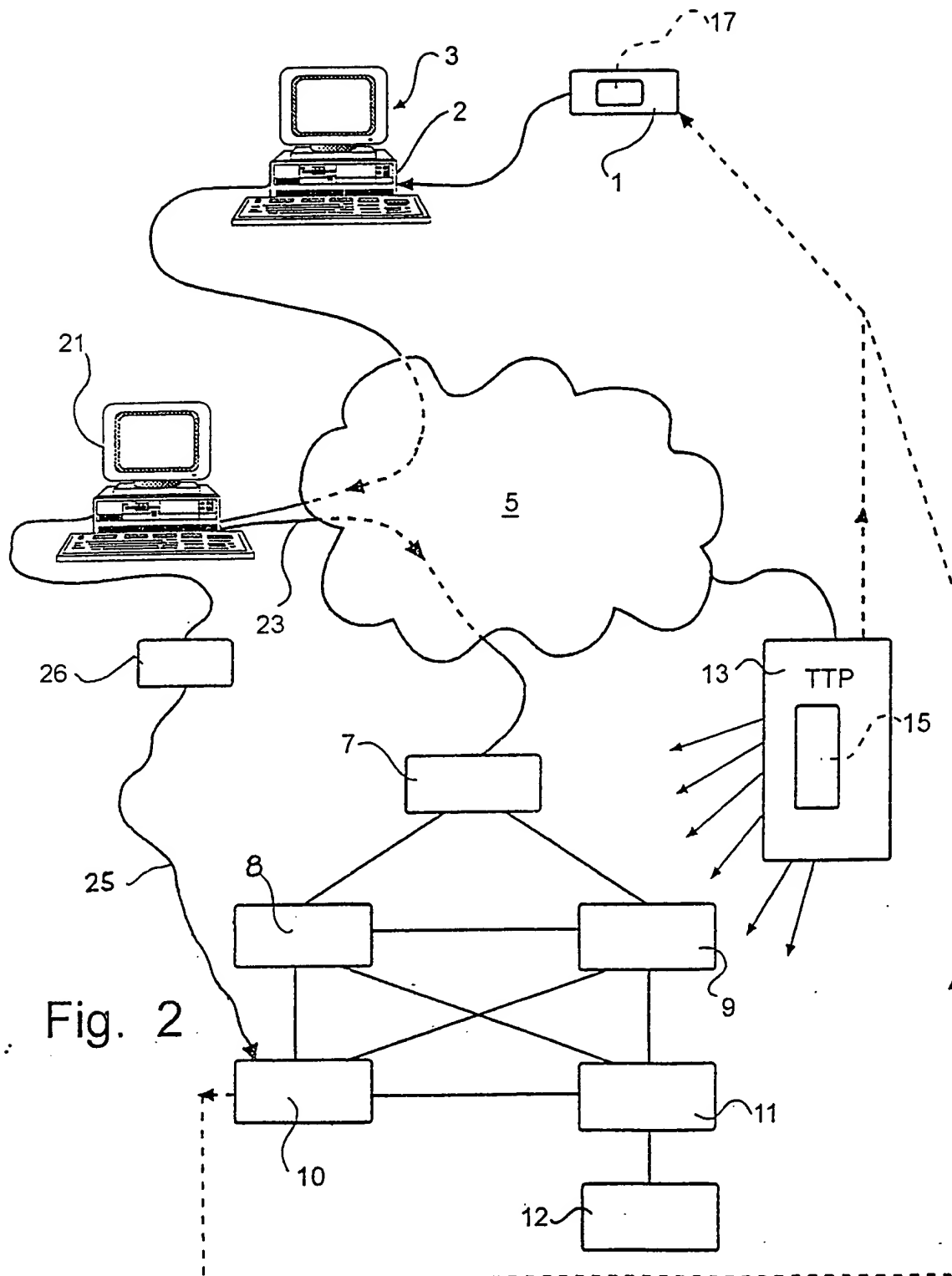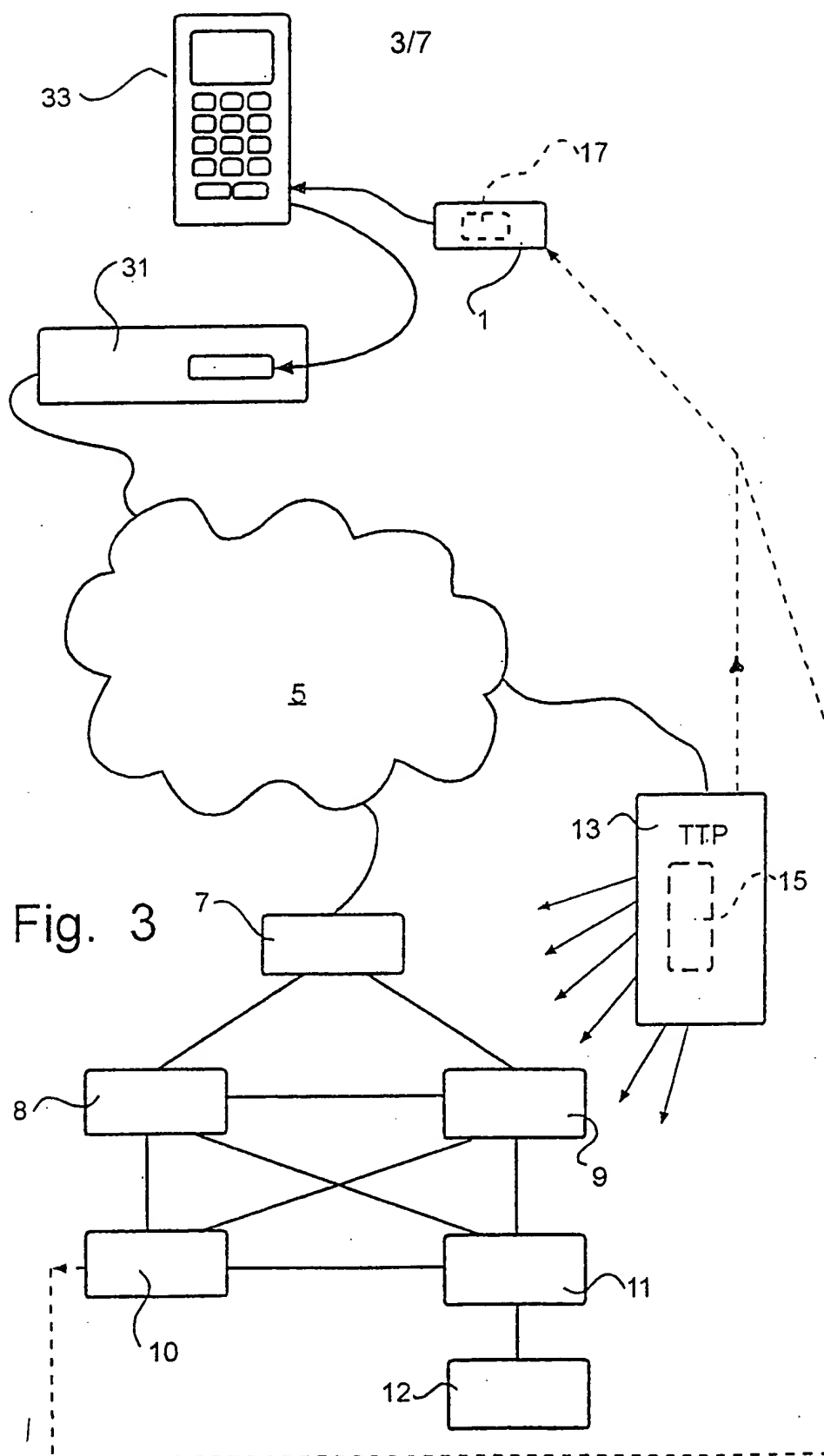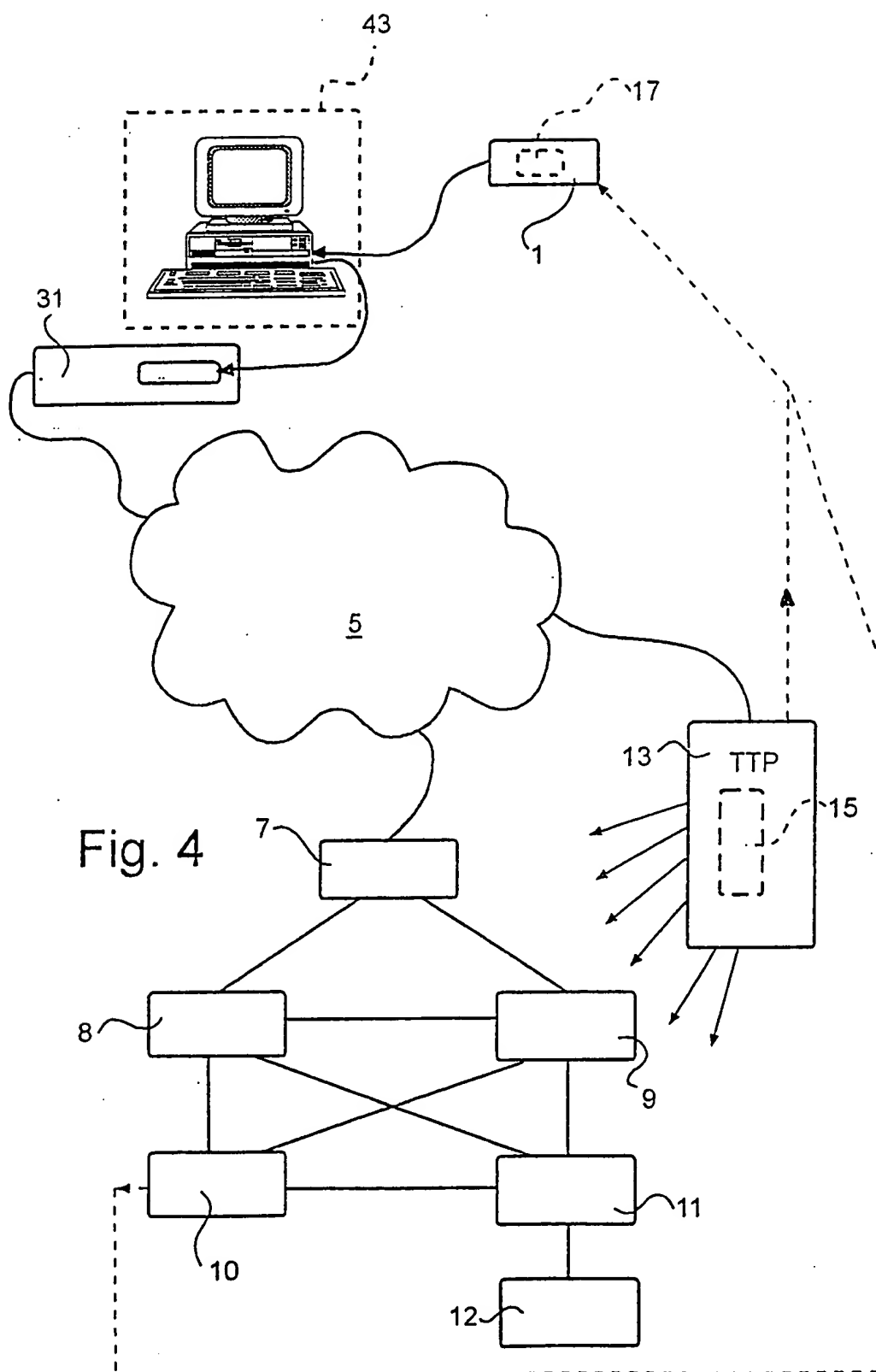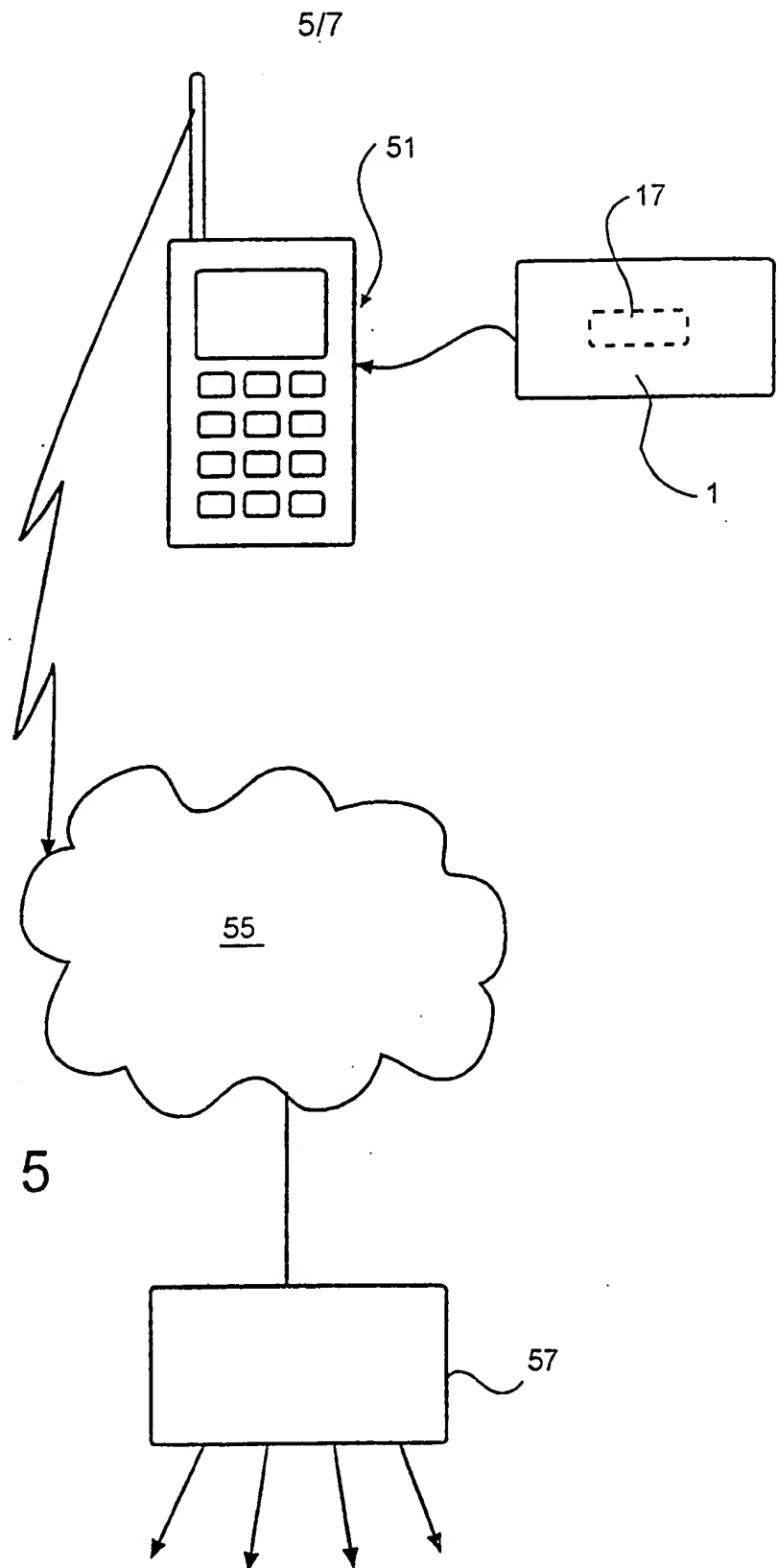with a digital signature based on the private key.

Fig. 1

Fig. 2

3/7

Fig. 3

Fig. 4

51

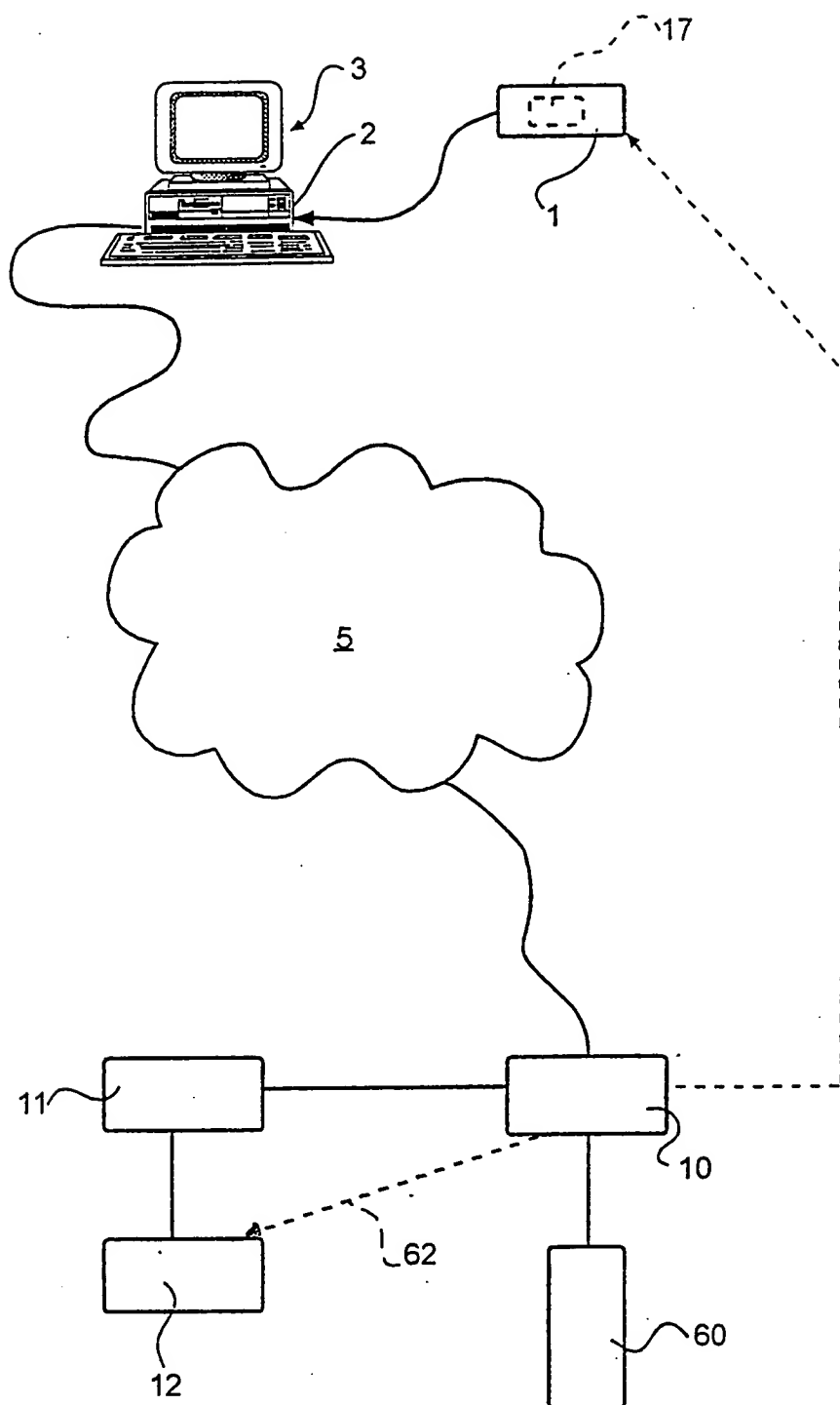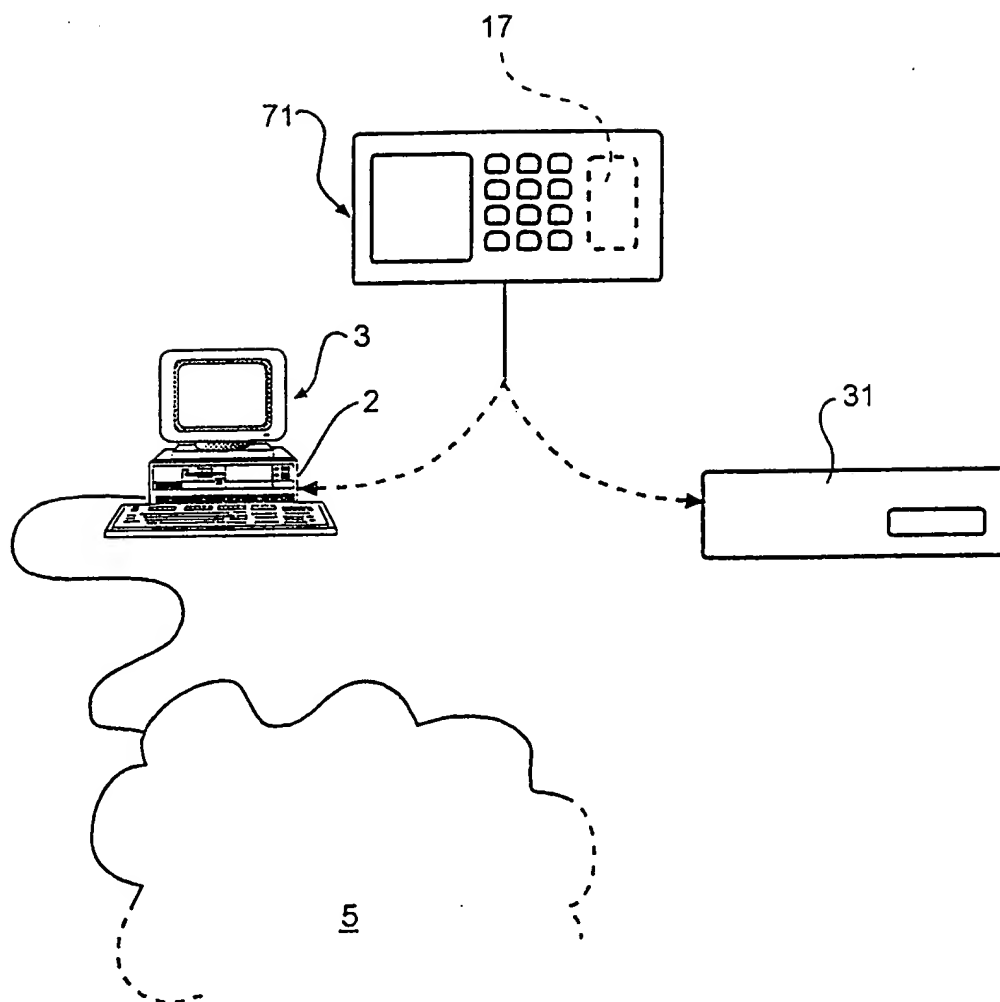17

1

55

Fig. 5

57
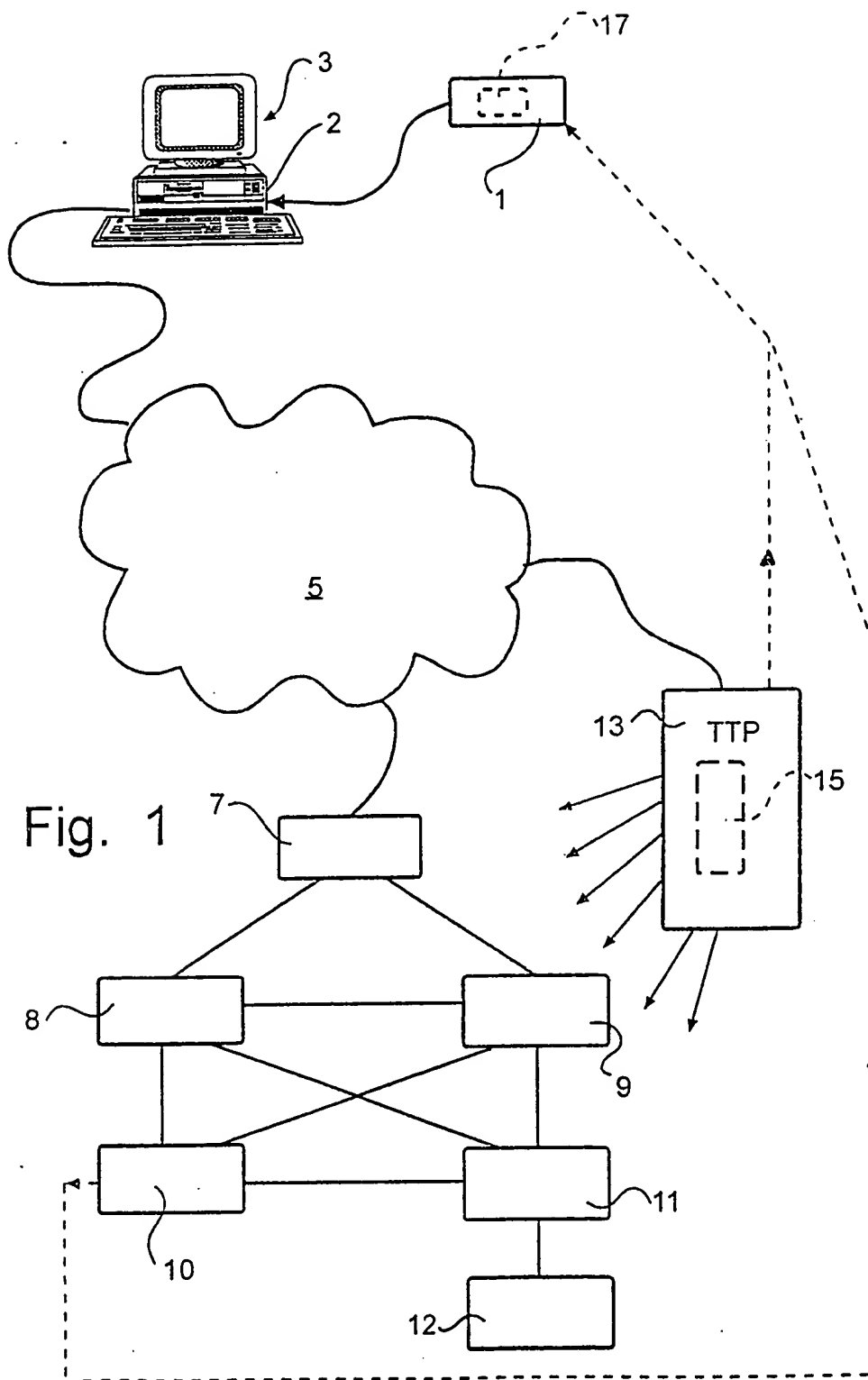
Fig. 6

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 98/00897

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06K 19/00, G07F 19/00, G07F 7/10, H04L 9/32, H04L 9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06K, G07F, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0214609 A2 (HITACHI, LTD.), 18 March 1987 (18.03.87), column 26, step 5010, column 28, step 5090, column 30, line 38 - line 46	1-4,10-20
Y		5-9
	--	
X	US 4926480 A (D. CHAUM), 15 May 1990 (15.05.90), column 7, line 1 - line 13, figure 1	21-26
Y		5-7
	--	
Y	US 5130519 A (G. BUSH ET AL), 14 July 1992 (14.07.92), column 5, line 49 - line 59, figure 2	8-9
A		21-26
	--	

X	Further documents are listed in the continuation of Box C.	X	See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" erlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 Sept. 1998	0 3 -09- 1998

Name and mailing address of the ISA	Authorized officer
Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Henrik Bodin Telephone No. +46 8 782 25 00

Form PCT ISA 210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/SE 98/00897

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0166541 A2 (KABUSHIKI KAISHA TOSHIBA), 2 January 1986 (02.01.86), abstract	1,21
A	EP 0385400 A2 (ATALLA CORPORATION), 5 Sept 1990 (05.09.90), abstract	1
A	US 5502765 A (G. ISHIGURO ET AL), 26 March 1996 (26.03.96), abstract	1,21-26
A	US 4849613 A (R.H. EISELE), 18 July 1989 (18.07.89), abstract	1-26
P,A	US 5721781 A (V. DEO ET AL), 24 February 1998 (24.02.98), abstract	1-26
E,A	WO 9825220 A1 (INSTITUTE OF SYSTEMS SCIENCE), 11 June 1998 (11.06.98), abstract	1-26

--

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0214609 A2	18/03/87	DE 3687934 A	15/04/93
		JP 62056043 A	11/03/87
		US 4885777 A	05/12/89
		US 5018196 A	21/05/91
US 4926480 A	15/05/90	AT 156639 T	15/08/97
		AU 3771489 A	12/12/89
		DE 68928240 D	00/00/00
		EP 0418328 A,B	27/03/91
		EP 0773647 A	14/05/97
		JP 3505032 T	31/10/91
		WO 8911762 A	30/11/89
		DE 3485804 A	13/08/92
		EP 0139313 A,B	02/05/85
		SE 0139313 T3	
		US 4759063 A	19/07/88
US 5130519 A	14/07/92	US 5265162 A	23/11/93
EP 0166541 A2	02/01/86	JP 61009052 A	16/01/86
		US 4823388 A	18/04/89
EP 0385400 A2	05/09/90	SE 0385400 T3	
		AU 615832 B	10/10/91
		AU 5052790 A	06/09/90
		CA 2010345 A	01/09/90
		DE 69019037 D,T	12/10/95
		JP 3067355 A	22/03/91
		US 4965568 A	23/10/90
US 5502765 A	26/03/96	EP 0588339 A	23/03/94
		JP 6103425 A	15/04/94
		US 5396558 A	07/03/95
		US 5446796 A	29/08/95
		JP 6103426 A	15/04/94
		JP 6162289 A	10/06/94
		JP 6162287 A	10/06/94
		JP 6161354 A	07/06/94
US 4849613 A	18/07/89	AU 573872 B	23/06/88
		AU 4538085 A	29/01/87
		DE 3417766 A	14/11/85
		DK 208185 A	13/11/85
		EP 0172314 A	26/02/86
		JP 61033574 A	17/02/86
US 5721781 A	24/02/98	NONE	
WO 9825220 A1	11/06/98	NONE	